Training: Threat Intelligence Reporting

The Threat Intelligence Reporting course has been designed for security professionals that need to learn how create and submit regular Threat Intelligence Reports (TIRs) to the Chief Information Security Officer or senior management. Leveraging the Enterprise Immune System's powerful machine learning and mathematics algorithms, participants will use the Threat Visualizer as a platform to carry out detailed Threat Hunting techniques and learn the craft of creating TIRs that highlight prioritized risks to the organization.

Participants have the opportunity to explore advanced models in greater depth and learn how to write their own Threat Intelligence Reports. This process requires a strong understanding about how to rank the most important model breaches and how to write a report to the desired standard and format. Attendees are tasked to evaluate which models are triggered by different threats and they must write their own report which is evaluated by the instructor.

Darktrace training courses are heavily oriented toward hands-on practical experience to reinforce formal classroom instruction. Using fast-track training methods, the majority of the training will take place in a workshop environment following preset training courses that will challenge the trainee and aid them during the learning process.

Course name: Threat Intelligence Reporting

Duration: 1 day

Audience: Network Security Professionals, Cybersecurity Analysts

Prerequisites: Participants must have attended the Threat Visualizer training course

Training Format: Practical Hand-on course 70%, Theory 30%

Course Outline: Threat Intelligence Reporting is a concise course that builds on knowledge gained from the Threat Visualizer course. This course is densely packed with all the fundamental information you need to start your Darktrace project

Training Objectives: Participants gain in-depth knowledge to better understand advanced models and it prepares participants to write their own Threat Intelligence Reports

Course Agenda

Training material is provided for each participant which set out the tasks and lessons planned. Key objectives include:

1. Learning Objectives

Introduction and welcome

2. Darktrace Detection Capabilities

Overview of latest Threat Visualizer updates and new functionality
Examples of recent breaches and new threats
Model changes and experimental Models
Introduction to Threat Intelligence Reports

3. Models

Types of Models
Process to create Models
Model configuration
Model Tuning
Examine Key models, metrics and filters
Exercise to explain how Models work
Exercise to understand how different threats trigger differ Models
Creating Advanced Models

4. Investigating Anomalies

Explore the Analyst Workflow
Threat Visualizer Analysis Levels
Metadata Analysis in Advanced Search
PCAP Analysis
Analyst Toolset
Exercise: Analyst questions
Exercise: Anomalous File Investigation

5. Threat Intelligence Reports

What is a TIR?
Threat Indicators
TIR Security
TIR Format
Executive Summary
Incident Summary
Incident Details
Exercise: Create a TIR
Present findings
TIR Evaluation

About Darktrace

Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 23 offices worldwide.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 20 7925 3551
Asia Pacific:+65 6248 4516

Email: info@darktrace.com

www.darktrace.com